STATE OF MONTANA
Department of Administration
INFORMATION TECHNOLOGY SERVICES DIVISION

Brian Schweitzer
Governor

Chief Information Officer

Advisory

December 5, 2006

To: Distribution

Subject: Exception to the Interim Policy: Security of Sensitive Data

---

Reference:

The Interim Policy: Security of Sensitive Data (http://itsd.mt.gov/policy/policies/Interim_Data_Security_Policy.pdf), Section IV.A.6:

Sensitive Data Shall:

6. Be encrypted when taken off State premises on…portable storage.

Request for Exception:

The Department of Administration/Information Technology Services Division (DOA/ITSD) has requested an exception to the policy requirement that portable storage media, in the form of computer backup tapes containing sensitive data, be encrypted when taken off State premises for transport to a secured storage facility.

At Issue:

Computer backup tapes typically contain sensitive data and are transported to secured locations for safe keeping or processing in the event of a recovery from an incident. The encryption of many hundreds of computer backup tapes per day would add significantly to agency daily batch processing times, would require additional processing resources, and would affect the ability to meet customer availability requirements. In the event of a recovery from a disaster or incident, a corresponding performance impact would adversely affect recovery time.

In addition, the State's disaster recovery contractor's equipment is not presently capable of processing encrypted tape cartridges. Requiring the contractor to acquire this capability would result in significant increases in contract costs.

The State of Montana Chief Information Officer (CIO) recognizes that this situation is not unique to any one agency and other agencies may be operating in similar circumstances. Therefore the CIO will grant an exception to all agencies that meet the conditions of the exception.

Exception Conditions:

The CIO will grant an exception for all organizations affected by the Interim Policy: Security of Sensitive Data with the following conditions:

1. The exception applies to portable storage media containing sensitive data; the exception does not apply to portable storage devices.
2. Portable storage media containing sensitive data may be taken off State premises un-encrypted under the following rules:
    a. The media shall be transported in locked cases, sealed with tamper-proof seals.
    b. Keys to the locked case(s) shall be transported separately from the case(s).
    c. During transport, the locked case(s) must be in the possession of either a state employee that has passed a fingerprint-based background check, or a bonded carrier. (The background check may be obtained from the State of Montana Department of Justice for a nominal fee.) A State of Montana fingerprint-based background check is the minimum requirement. A national fingerprint-based

background check is required if the sensitive data on the portable storage media is Criminal Justice Information Network-related.

d. The current location of the transport cases may be readily discerned and tracked.

3. An agency wanting to take advantage of this exception must:
   - Notify the CIO Policy Team at ITPolicy@mt.gov. Notification must come from the department head.
   - Provide a point of contact within the agency.
   - Provide a documented procedure describing the handling of portable storage media under this exception.

Adherence to these conditions constitutes compliance to the encrypted portable media requirement, Section IV.A.6, for the Interim Policy: Security of Sensitive Data. All other requirements of the policy remain in force.

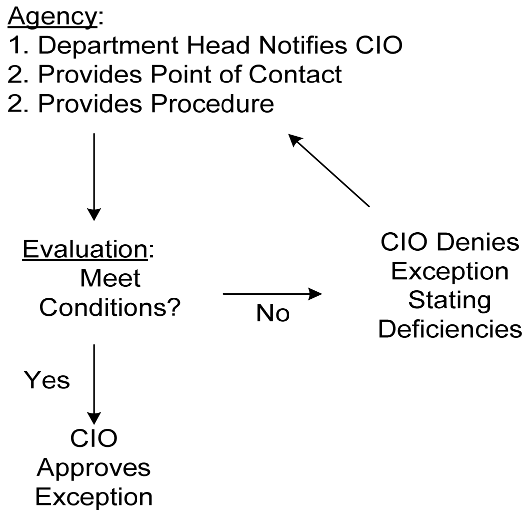
To Receive An Exception:

The granting of exceptions shall be accomplished by the following steps:

1. If an agency wishes to obtain an exception; the agency shall implement the prescribed terms and conditions and provide requested documentation to the CIO (at ITPolicy@mt.gov). If the situation does not apply to the agency, no action is required.
2. The documentation shall be evaluated by the CIO and the Office of Cyber Protection.
3. If the documentation meets the terms and conditions of the exception; the CIO shall approve the exception for the agency and notify the agency in writing.
4. If the documentation does not meet the terms and conditions; the CIO shall document and communicate the deficiencies back to the agency.

These steps are shown in the following graphic:

Exception Approval Steps


Agency:
1. Department Head Notifies CIO
2. Provides Point of Contact
2. Provides Procedure
Evaluation:
Meet Conditions?
No
CIO Denies Exception Stating Deficiencies
Yes
CIO Approves Exception

Authority to Grant Exceptions:

The authority to grant or deny exceptions to statewide information technology (IT) policies and standards is vested in the State CIO under the terms of the statewide IT policy: Establishing and Implementing Statewide Information Technology Policies and Standards (the Enabling IT Policy) and its associated procedure.

If you have questions or comments, please feel free to contact the CIO Policy Team at (406) 444-2700 or ITPolicy@mt.gov.

To subscribe to automatic Enterprise IT publications notification, please visit:

http://itsd.mt.gov/policy/itpubnotify.asp

To subscribe to automatic CIO Advisory notification, please visit:

http://itsd.mt.gov/policy/advisories/cionotify.asp

Advisory Disposition: Retain until rescinded by policy or State CIO.

CIO_ADVRY_20061205